DOE CIO Guidance CS-38

U.S. Department of Energy

Cyber Security Program

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION GUIDANCE

July 20, 2006

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guidance applies the Office of Management and Budget (OMB) memorandum, M-06-16, *Protection of Sensitive Agency Information*, and the sections of OMB memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information technology Investments*, pertaining to the protection of personally identifiable information (PII).

   The DOE CIO will review this Guidance annually and update it as necessary. Senior DOE Management and their operating units may provide feedback at any time for incorporation into the next scheduled update.

   Attachment 2 contains the OMB definition of PII that should be used to implement this Guidance.

2. SCOPE.

   This Guidance provides additional information for the protection of PII in all information systems operated by the Department and its contactors.

3. CANCELLATIONS.

   None.

4. APPLICABILITY.

   a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-38 is Applicable.*

      Further, the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incorporated into contracts.

   b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information,* and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual,* provide additional information for identifying unclassified information requiring protection.

d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security systems. Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; DOE CIO Guidance CS-22, *National Security Systems Controls Guidance;* and NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System,* provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective upon issuance. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 30 days of its effective date.

This implementation of this guidance for the protection of PII on all Federal information systems must be completed by August 9, 2006, to be consistent with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information,* dated June 23, 2006.

6. CRITERIA.

a. Program Cyber Security Plan. Senior DOE Management PCSPs are to direct operating units to develop, document, and implement PII policies and procedures consistent with criteria b. through e. immediately below.

b. Use of Encryption

Implement the use of FIPS 140-2 Level 1 or higher encryption to protect all PII on laptops and on removable media, such as CDROMs or thumb drives.

- All laptop computers used by Federal employees and contractors who support Federal systems that contain PII should have an installed capability to encrypt all PII.
- All users of these laptops should be instructed to use this capability to protect all PII.

The following steps are to be followed to implement the criteria in this section:

- Identify all laptops that contain PII.
- Remove PII from all laptops for which its presence is not essential.
- Install encryption software for all laptops that will continue to contain PII or that will contain PII in the future.
- Provide training to the user(s) on the use of the encryption software.
- Provide direction to the user(s) that the encryption software is to be used to protect all PII on the laptop.

It is recommended that the use of encryption protection be applied to laptops and all desktop computer systems as well, so as to provide increased protection against loss of portable devices and cyber attacks.

c. Two Factor Authentication

Use two-factor authentication for all individuals having remote access to PII other than their own.

d. Remote Access

Ensure that a time-out function is in place on all systems supporting remote access that requires re-authentication of remote users if there is a period of 30 minutes or longer of inactivity on their connection to the system.

e. Management of PII on Laptops and Removable Media

Establish and implement procedures throughout the organization so that any files containing PII on laptops or removable media have been deleted, within 90 days, or that use of these files is still required.

Procedures are to include documentation of the regular use of these procedures for each laptop or removable media device that contains PII.

f. Reporting of Incidents Involving PII

Ensure that all suspected or confirmed cyber security and physical security incidents involving PII are reported to the DOE Cyber Incident Advisory Capability (CIAC) within 45 minutes of discovering the incident. CIAC is to report the incident to US-CERT within one hour of discovery of the incident.

When reporting incidents as possibly involving PII, there should be sufficient reason to believe that a security breech has occurred and that PII is likely to have been involved. Otherwise, the incident should be reporting following documented procedures for reporting all cyber security incidents.

Reports to CIAC may be made via email to ciac@ciac.org, by phone to 925-422-8193 or by fax to 925-423-8002.

CIAC will report the incident involving PII to the US-Computer Emergency Readiness Team (US-CERT).

7. RESPONSIBILITIES.

It is expected that Heads of Departmental Elements will be given delegated authority from the Deputy Secretary in the near future relative to determining that data on mobile computers/devices are non-sensitive (Recommendation 1 in OMB M-06-16).

8. REFERENCES.

References are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

9. DEFINITIONS.

Definitions specific to this Guidance are defined in Attachment 2. Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

10. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-38 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

GLOSSARY

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.